UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,212	03/30/2004	Iyad Qumei	200701958-2	4068

22879 7590 03/17/2011
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/17/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

____

Ex parte IYAD QUMEI

____

Appeal 2009-006597
Application 10/813,212[1]
Technology Center 2400

____

Before JOSEPH L. DIXON, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges.*

HUGHES, *Administrative Patent Judge.*

DECISION ON APPEAL[2]

[1] Application filed March 30, 2004, claiming priority to Provisional Application Serial No. 60/495091 filed March 31, 2003. The real party in interest is Hewlett-Packard Development Co., L.P. (App. Br. 2.)

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellant appeals from the Examiner's rejection of claims 1-41 under authority of 35 U.S.C. § 134(a). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellant's Invention

The invention at issue on appeal relates to a software and firmware updating device, method, and related network for updating software and/or firmware resident in a networked device, at least a portion of the software or firmware being encrypted. (Spec. ¶¶ [0008], [0010].)[3]

Representative Claim

Independent claims 1, 22, and 31 further illustrate the invention, and are reproduced below with the key disputed limitations emphasized:

> 1. An electronic device network for *updating at least one of firmware and software in a plurality of electronic devices* using at least one electronic device update, the network comprising:
>
> *at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine*;
>
> at least one update store storing a plurality of electronic device updates;
>
> at least one update delivery server adapted to dispense the plurality of electronic device updates; and

[3] We refer to Appellant's Specification ("Spec."); Appeal Brief ("App. Br.") filed April 3, 2008; and Reply Brief ("Reply Br.") filed August 20, 2008. We also refer to the Examiner's Answer ("Ans.") mailed June 23, 2008.

wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted.

22. An electronic device employing one of encrypting and decrypting techniques to update firmware and software, the electronic device comprising:

random access memory; and

non-volatile memory, the non-volatile memory comprising:

an update agent;

a first in first out (FIFO) memory device;

a firmware;

a software application; and

an update, *wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion.*

31. A method of building a firmware upgrade for use in an electronic device incorporating encryption, the method comprising:

building a firmware image to be encrypted, the firmware image comprising a plurality of components; and

encrypting the components before assembling the components into an encrypted firmware image.

References

The Examiner relies on the following references as evidence of unpatentability:

Nachenberg	US 6,230,316 B1	May 8, 2001

Selkirk	US 2003/0051160 A1	March 13, 2003

Rejections on Appeal

The Examiner rejects claims 1, 2, 4-9, 12, 22-28, 30, 31, and 41 under 35 U.S.C. § 102(a) as being anticipated by Selkirk.[4]

The Examiner rejects claims 10, 11, and 32-38 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Selkirk and Nachenberg.[5]

ISSUES

Based on our review of the administrative record, Appellant's contentions, and the Examiner's findings and conclusions, the pivotal issues before us are as follows:

1. Does the Examiner err in finding Selkirk discloses: (1) an "update generator . . . comprising an encrypting and decrypting engine;" and (2) "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted" as recited in Appellant's claim1?

[4] The Final Office Action mailed November 23, 2007 rejects claims 1-9 and 12 under 35 U.S.C. § 102(a) as anticipated by Selkirk; and rejects claims 10, 11, and 13-41 under 35 U.S.C. § 103(a) as being unpatentable over Selkirk and Nachenberg. (Final Rejection at pp. 2, 5.) The Examiner's Answer withdraws the rejection of claims 3, 13-21, 29, 39, and 40 (Ans. 3-4), and revises the basis for rejecting claims 22-28, 30, 31, and 41 (previously § 103(a), now § 102(a)) (Ans. 5).

[5] *See* Note 4 (*supra*) – claims 22-28, 30, 31, and 41 were previously rejected under 35 U.S.C. § 103(a).

2. Does the Examiner err in finding Selkirk discloses: (1) a "non-volatile memory . . . comprising . . . a first in first out (FIFO) memory device;" and (2) "wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion" as recited in Appellant's claim 22?

3. Does the Examiner err in finding Selkirk discloses "building a firmware image to be encrypted, the firmware image comprising a plurality of components; and encrypting the components before assembling the components into an encrypted firmware image" as recited in Appellant's claim 31?

FINDINGS OF FACT (FF)

Selkirk Reference

1. Selkirk generally describes a firmware device and method for downloading data from a network server to a firmware device. Selkirk describes a computer sending

> a request to a server to download the particular data to a particular firmware device. The server contacts the firmware device directly through the network to initiate the transfer. The server and firmware device communicate over an encrypted data channel so as to prevent any third party, including the aforementioned computer, from intercepting and storing the transmitted data.

(¶ [0009].) The downloaded data may be an update to firmware. (¶ [0008].)

2. Selkirk also describes, with respect to Figure 1, transferring a firmware update. A computer (102) communicates with a server (106) and a

firmware device (108), which may be located within computer. The computer requests an update to the firmware device – in this example, the computer's firmware – from the server, and the server "sends the data over an encrypted communications channel to the firmware device 108, where the data is decrypted. No decryption of the data takes place outside of firmware device 108. . . . [O]nly [the] firmware device 108 can decrypt the encrypted transmission." Preferably, the encrypted communications channel utilizes "the Secure Sockets Layer (SSL) protocol." (¶ [0017]; Fig. 1.)

3. Selkirk further describes a firmware device (108), including an embedded processor (200B) receiving instructions from cryptographic program memory (204B) through internal bus (202B), and also sending data to and receiving data from the computer (102) through external bus interface (206B) and external bus (208B). (¶ [0023]; Fig. 2B.) "Firmware memory 210B . . . provides storage for the actual firmware (i.e., the code and data to be used by the computer or peripheral." (¶ [0024] (emphasis added).)

4. Selkirk further explains that "SSL must rely on some form of public-key cryptography [(cryptosystems or 'cipher suites')] in its handshake procedure." The cipher suites supported by SSL include:

> DES (data encryption standard), 3DES (triple DES), DSA (digital signature algorithm), KEA (key exchange algorithm), MD5 (message digest algorithm 5), RC2 (Rivest cipher 2), RC4 (Rivest cipher 4), RSA (Rivest, Shamir, and Adleman) public-key algorithm, RSA key exchange, SHA-1 (secure hash algorithm), and SKIPJACK. . . . RSA is commonly used for handshaking, and RC4 is commonly used for data transmission, for example.

(¶ [0034].)

ANALYSIS

Appellant has the opportunity on appeal to the Board of Patent Appeals and Interferences (BPAI) to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) (citing *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). The Examiner sets forth a detailed explanation of a reasoned conclusion of anticipation in the Examiner's Answer with respect to Appellant's claims 1, 2, 4-9, 12, 22-28, 30, 31, and 41 (Ans. 5-8, 12-14), and in particular independent claims 1, 22, and 31 (Ans. 5-6, 8, 12-14). The Examiner also sets forth a detailed explanation of a reasoned conclusion of obviousness in the Examiner's Answer with respect to Appellant's claims 10, 11, and 32-38. (Ans. 9-11, 13-15.) Therefore, we look to the Appellant's Briefs to show error in the proffered reasoned conclusions. *See Kahn*, 441 F.3d at 985-86.

Arguments Concerning the Examiner's Rejection of Representative Claim 1 and Claims 2, 4-9, and 12

The Examiner rejects Appellant's independent claim 1 as being anticipated by Selkirk. (Ans. 5-6.) Appellant contends that Selkirk does not anticipate representative claim 1 (App. Br. 7-15), which calls for, in pertinent part: (1) an "update generator . . . comprising an encrypting and decrypting engine;" and (2) "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted" (App. Br. 22, Claim App'x., Claim 1). Based on the record before us, we find error in the Examiner's anticipation rejection of Appellant's claim 1. We agree with Appellant that Selkirk does not disclose the disputed features of at least (1) an update generator comprising an encrypting and decrypting engine, and (2) at least a portion of the firmware or software in the electronic devices is encrypted for essentially the reasons espoused by Appellant. (App. Br. 7-15; Reply Br. 2-6).

The Examiner finds that Selkirk discloses each feature of Appellant's claim 1, including: "at least one update generator comprising an encrypting and decrypting engine" (citing ¶ [0017]); and "wherein at least one of the firmware and software in the plurality of electronic devices and the at least one update being encrypted" (citing ¶¶ [0009], [0017]). (Ans. 5.) Additionally, the Examiner responds that

> Selkirk discloses that a client/firmware device requests firmware update from a server and the server generates encrypted firmware update and provides it to the firmware device. Therefore, although Selkirk does not disclose in detail generation of the update, paragraph [0017] provides sufficient information pertaining to generation of firmware update as coming from the server which implies that the server is responsible for generation of the update.

(Ans. 12-13 (citation omitted).)

The Examiner also responds that

> The examiner has relied on the Selkirk reference to disclose securely transmitting encrypted firmware update from server to client and no decryption of the encrypted firmware update takes place outside of the firmware device (. . . the firmware update is a portion of the firmware and software of the electronic device). Therefore, when the firmware device receives firmware update/portion of the firmware and software in the electronic device, the firmware update is in encrypted state prior to decryption.

(Ans. 12.)

As explained by Appellant, claim 1 includes a limitation requiring "at least one update generator comprising an encrypting and decrypting engine." (App. Br. 11.) Selkirk, on the other hand, describes that "an update to firmware may be downloaded . . . . [but,] Selkirk provides no details as to how the update came to exist, or how the server 106 came into possession of the update, and certainly fails to describe, teach or suggest that the server 106 generated the update." (App. Br. 14-15 (*see* App. Br. 11-12; Reply Br. 5-6).)

As further explained by Appellant, claim 1 recites the limitation of "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted" (App. Br. 9); however, "Selkirk merely discloses that data is sent over an encrypted channel to a firmware device, where the data is decrypted." (App. Br. 13; *see* App. Br. 10-12, 14.) Specifically, Appellant contends that: "a <u>firmware device</u> and a <u>firmware update</u> are quite different from the <u>firmware itself</u> in an electronic device" (Reply Br. 3); Selkirk describes "a clear distinction between firmware and a firmware <u>device</u>" (Reply Br. 4); and "because the file of Selkirk is decrypted <u>before</u> the firmware device stores the file, and because Selkirk states that the 'actual firmware' is <u>stored</u> in 'firmware memory 210B,' Selkirk does not disclose" (Reply Br. 5) the disputed limitation of at least a portion of the firmware or software being encrypted. "Instead, in Selkirk, an encrypted file is decrypted before it is stored and can become a part of the actual firmware" (Reply Br. 5). (*See* Reply Br. 2-6.)

As detailed in the Findings of Fact section *supra*, we agree with the Examiner that Selkirk discloses transferring data to a firmware device over an encrypted communications channel, that the data may be an update to the firmware, that the firmware device decrypts the transferred data, and that an encrypted SSL communications channel "implies" generating encrypted data and decrypting the encrypted data after transfer completion. (FF 1, 2; *see*

Ans. 5-6, 12-13.) We, however, also agree with the Examiner that "Selkirk does not disclose in detail generation of [a firmware and/or software] update." (Ans. 13.) We therefore disagree with the Examiner's conclusion that Selkirk "provides sufficient information pertaining to generation of firmware update as coming from the server which implies that the server is responsible for generation of the update." (Ans. 13.)

Although Selkirk discloses a "client/firmware device request[ing] [a] firmware update from a server," we do not agree that "the server generates [an] encrypted firmware update and provides it to the firmware device." (Ans. 13.) We do not readily find any description in Selkirk of the server actually generating a firmware update or encrypting/decrypting the firmware update. At most, Selkirk discloses the server encrypting data (a message or data packet), transferring the encrypted data to a firmware device, and the firmware device decrypting the data. (*See, e.g.*, Selkirk ¶¶ [0025]-[0026].) Appellant's claim 1, however, recites an "update generator . . . comprising an encrypting and decrypting engine" separate from an update delivery server, which may include an SSL layer. (*See*, *e.g.*, Spec. [0008]-[0010]; [0063]-[0065]; Fig. 2.) Thus, we are constrained by the record before us to agree with Appellant that Selkirk does not disclose at least the disputed feature of an "update generator . . . comprising an encrypting and decrypting engine."

We also agree with the Examiner that Selkirk discloses data transfer of a firmware update or software over an encrypted SSL communications channel. (FF 1, 2.) We, however, disagree with the Examiner's conclusion that Selkirk discloses "wherein at least one of the firmware and software in the plurality of electronic devices and the at least one update being encrypted" (Ans. 5), based on Selkirk's disclosure that "when the firmware device receives firmware update/portion of the firmware and software in the electronic device, the firmware update is in encrypted state prior to decryption" (Ans. 12).

We give claim terminology the "broadest reasonable interpretation consistent with the [S]pecification" in accordance with our mandate that "claim language should be read in light of the [S]pecification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations omitted). We must, however, avoid importing limitations from Appellant's Specification. *Superguide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("Though understanding the claim language may be aided by explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim.").

Here, claim 1 recites "a portion of the . . . firmware [or] software in the . . . electronic devices is encrypted." Appellant explains that the firmware or software to be updated is resident in (a part of) the device and that the update is encrypted/decrypted separately from the firmware. (Spec. [0060], [0063], [0065].) Appellant also explains (*supra*) that Selkirk distinguishes a firmware device from the firmware code itself. (FF 3.) While we must be mindful of reading in limitations from the Specification, in view of Appellant's and Selkirk's disclosures we disagree with the Examiner's conclusion that Selkirk discloses encrypting a portion of the firmware itself or a portion of the software resident in the device. At most, Selkirk discloses the server encrypting data and the firmware device decrypting the data (data packet) (*supra*). We do not readily find any description in Selkirk of firmware in the device, or any software in the device being encrypted. An encrypted data packet containing a portion of firmware or software code, as described by Selkirk, is not equivalent to a portion of encrypted firmware or software resident in an electronic device, as required by Appellant's claim. Thus, we are constrained by the record before us to agree with Appellant that Selkirk does not disclose at least the disputed feature of "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted."

Appellant's claims 2, 4-9, and 12 depend on claim 1, and stand with representative claim 1. Thus, based on the record before us, we find that the Examiner erred in finding Selkirk discloses each limitation recited in Appellant's claims 1, 2, 4-9, and 12. Accordingly, we reverse the Examiner's anticipation rejection of these claims.

The Examiner's Rejection of Claims 22-38, and 30 Under 35 U.S.C. § 102(a)

The Examiner rejects Appellant's independent claim 22 which calls for, in pertinent part: (1) a "non-volatile memory . . . comprising . . . a first in first out (FIFO) memory device;" and (2) "wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion" (App. Br. 27, Claim App'x., Claim 22). The Examiner rejects Appellant's independent claim 22 as being anticipated by Selkirk. (Ans. 5, 8.) Specifically, the Examiner finds that "claim[s] 22-28 and 30 encompass the same scope as claims 1, 2, 4-9 and 12. Therefore, claims 22-

28 are rejected based on the same reason set forth above in rejecting claims 1, 2, 4-9 and 12." (Ans. 8.) Additionally, the Examiner responds that:

> Selkirk discloses the firmware memory is connected to internal bus and provides storage for the actual firmware and is preferably some kind of write-able non-volatile memory such as EEPROM, flash ROM and non-volatile RAM (Selkirk: [0024]). Therefore, although no specific word mentions "FIFO" and FIFO memory does not appears to be a patentable feature, the memory device disclosed by Selkirk discloses the hardware limitation disclosed by appellant. In addition, the claim only recites of a FIFO memory device but fails to distinguish how the FIFO is used in relation to updating of firmware.

(Ans. 13-14.)

Appellant contends that Selkirk does not anticipate (nor render obvious) representative claim 22 (App. Br. 8, 17-18; Reply Br. 6-7.)

Based on the record before us, we find error in the Examiner's anticipation rejection of Appellant's claim 22. We agree with Appellant that Selkirk does not disclose the disputed features of at least (1) non-volatile FIFO memory, and (2) an encrypted portion of at least one of the firmware and the software application selected for updating for essentially the reasons espoused by Appellant. (App. Br. 17-18; Reply Br. 6-7.)

We find that the Examiner's rejection is facially insufficient, and that the Examiner has failed to present a prima facie anticipation rejection for claims 22-28 and 30. Even a cursory reading of representative claim 22 demonstrates that the claim has a very different scope from representative claim 1. The claim is directed to a device, and recites a number of structural limitations, including a non-volatile FIFO memory. We disagree with the Examiner that Selkirk discloses such a memory. In particular, we disagree with the Examiner that Selkirk's disclosure of "firmware memory . . .

[which] is preferably some kind of write-able non-volatile memory such as EEPROM, flash ROM and non-volatile RAM" (Ans. 13) is equivalent to a non-volatile FIFO memory. Although Selkirk describes non-volatile memory, the disclosed EEPROM, flash ROM, and non-volatile RAM are all addressable memory (e.g., RAM (Random Access Memory)), not FIFO memory. Moreover, as explained with respect to claim 1 (*supra*), Selkirk does not disclose encrypted firmware or software. Thus, we are constrained by the record before us to agree with Appellant that Selkirk does not disclose at least the disputed feature of (1) a "non-volatile memory . . . comprising . . . a first in first out (FIFO) memory device;" and (2) "wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating, and wherein updating at least one of the firmware and the software application comprises decrypting the encrypted portion."

Appellant's claims 23-28 and 30 depend on claim 22, and stand with representative claim 22. Thus, based on the record before us, we find that the Examiner erred in finding Selkirk discloses each limitation recited in Appellant's claims 22-28 and 30. Accordingly, we reverse the Examiner's anticipation rejection of these claims.

Arguments Concerning the Examiner's Rejection of Representative Claim 31 and Claim 41

The Examiner rejects Appellant's independent claim 31 which calls for, in pertinent part, "building a firmware image to be encrypted, the firmware image comprising a plurality of components; and encrypting the components before assembling the components into an encrypted firmware image" (App. Br. 29, Claim App'x., Claim 31). The Examiner rejects

Appellant's independent claim 31 as being anticipated by Selkirk. (Ans. 5, 8.) Specifically, the Examiner finds that "the firmware image compris[es] a plurality of components[ ] and encrypting the components before assembling the component[s] into an encrypted firmware image (Selkirk: [0034]: encryption utilizes RC4/symmetric stream cipher that performs encryption using keystream through bit-wise operation so that components of firmware update encrypted before assembly)." (Ans. 8.) Additionally, the Examiner responds that:

> Selkirk discloses that firmware update is subject to encryption and the encryption preferably uses RC4 cipher/stream cipher or DES/block cipher that encrypts data by performing encryption block by block/component by component (Selkirk: [0034]). Therefore, the components of firmware update are encrypted prior to being assembled into an update packet.

(Ans. 14.)

Appellant contends that Selkirk's disclosure of handshaking and/or data transmission cipher suites (e.g., RC4, and DES) utilized in an SSL channel does not disclose "'block by block' or 'component by component' encryption" (Reply Br. 8), and in any event does not disclose "encrypting the components before assembling the components into an encrypted firmware image" as required by claim 31.

Based on the record before us, we find error in the Examiner's anticipation rejection of Appellant's claim 31. We agree with Appellant that Selkirk does not disclose the disputed features, and that the Examiner's rejection is insufficient to present a prima facie case for anticipation. Specifically, Selkirk only describes handshaking and/or data transmission cipher suites (e.g., RC4, and DES) utilized in an SSL encrypted communications channel. (FF 4.) We do not readily find any description of "block by block" encryption as asserted by the Examiner (Ans. 14). To the extent Examiner asserts such block by block encryption is inherent in Selkirk's description of SSL cipher suites, we find this to be an unsupported finding of inherency. Moreover, Appellant's claim 31 does not recite encrypting the data packet including the firmware update (*see* discussion of claim 1, *supra*) using component by component encryption. Rather, claim 31 recites encrypting components before assembling them into an encrypted firmware image – it is this encrypted image that is transmitted (e.g., as an encrypted data packet over an SSL channel) (*see*, *e.g.*, Spec. ¶¶ [0064]-[0065]; [0082], [0085]). Thus, we are constrained by the record before us to agree with Appellant that Selkirk does not disclose at least the disputed feature of "encrypting the components before assembling the components into an encrypted firmware image" as recited in representative claim 31.

Appellant's claim 41 depends on claim 31, and stands with representative claim 31. Thus, based on the record before us, we find that the Examiner erred in finding Selkirk discloses each limitation recited in Appellant's claims 31 and 41. Accordingly, we reverse the Examiner's anticipation rejection of these claims.

The Examiner's Rejection of Claims 10, 11 and 32-38 Under 35 U.S.C. § 103(a)

The Examiner rejects Appellant's dependent claims 10, 11, and 32-38 as being unpatentable over the combination of Selkirk and Nachenberg. (Ans. 9-11; *see* note 5 (*supra*).) Claims 10 and 11 depend on claim 1. Claims 32-38 depend on claim 31. For the reasons explained with respect to claim 1 and claim 31 (*supra*), we find Selkirk does not disclose, teach, or suggest each feature of these claims. Nachenberg does not cure the deficiencies of Selkirk. Therefore, based on the record before us, we find that the Examiner erred in finding Selkirk and Nachenberg would have collectively taught or suggested each limitation recited in Appellant's claims 10, 11, and 32-38. Accordingly, we reverse the Examiner's obviousness rejection of these claims.

CONCLUSIONS OF LAW

Appellant has shown that the Examiner erred in rejecting claims 1, 2, 4-9, 12, 22-28, 30, 31, and 41 under 35 U.S.C. § 102(a).

Appellant has shown that the Examiner erred in rejecting claims 10, 11, and 32-38 under 35 U.S.C. § 103(a).

DECISION

We reverse the Examiner's rejection of claims 1, 2, 4-9, 12, 22-28, 30, 31, and 41 under 35 U.S.C. § 102(a).

We reverse the Examiner's rejection of claims 10, 11, and 32-38 under 35 U.S.C. § 103(a).

REVERSED

msc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS CO 80528